

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

REC'D 20 DEC 2005

WIPO



PCT

Applicant's or agent's file reference DE920030011	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP2004/050864	International filing date (day/month/year) 19.05.2004	Priority date (day/month/year) 11.07.2003
International Patent Classification (IPC) or both national classification and IPC H04L29/06		
Applicant INTERNATIONAL BUSINESS MACHINES CORPORATION et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 5 sheets, including this cover sheet.
 - ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 7 sheets.

3. This report contains indications relating to the following items:
 - I ☒ Basis of the opinion
 - II ☐ Priority
 - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
 - IV ☐ Lack of unity of invention
 - V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
 - VI ☐ Certain documents cited
 - VII ☐ Certain defects in the international application
 - VIII ☐ Certain observations on the international application

Date of submission of the demand 21.04.2005	Date of completion of this report 20.12.2005
Name and mailing address of the international preliminary examining authority:  European Patent Office - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Authorized Officer Adkhis, F Telephone No. +31 70 340-4241 

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/EP2004/050864

I. Basis of the report

1. With regard to the **elements** of the international application (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17):*

Description, Pages

1, 2, 4-15 as originally filed
3, 3a received on 21.04.2005 with letter of 15.04.2005

Claims, Numbers

1-16 received on 21.04.2005 with letter of 15.04.2005

Drawings, Sheets

1/9-9/9 as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language: , which is:

- ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☒ the claims, Nos.: 17-20
- ☐ the drawings, sheets:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. **PCT/EP2004/050864**

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	1-16
	No: Claims	
Inventive step (IS)	Yes: Claims	1-16
	No: Claims	
Industrial applicability (IA)	Yes: Claims	1-16
	No: Claims	

2. Citations and explanations

see separate sheet

1. The invention discloses a method (**independent claim 7**) for authenticating clients in a client-server environment, wherein said client-server environment uses a communication protocol that allows extensions of the header request without violating said communication protocol, wherein a system establishes communication between said client and said server, wherein said system comprises the steps of: receiving a header request from said client, inserting authentication information into said header request resulting in an extended header request independently of the authentication process used by said server and without server requesting authentication information, sending said extended header request to a server and receiving information from said server if the authentication has been successful. The corresponding method implemented at the client-side (**independent claim 1**), the corresponding method implemented at the server-side (**independent claim 10**) and the corresponding server system (**independent claim 12**), client system (**independent claim 13**) and proxy server system (**independent claim 15**) are also disclosed.

2. Such methods and systems are disclosed in the closest prior art D1= US2002/0133700.

2.1 The difference between the document D1 and the invention is the following:

The inserted authentication information comprises the client certificate containing client's name and client's public key, and a digital signature which has been generated over the whole header request including client certificate using client's private key.

2.2 The problem solved by such a technical feature is how to ensure that the client is securely authenticated without the need of a secure protocol like SSL. More specifically how to ensure that the request header arriving at the server has not been tampered with on the way from the client to the server.

2.3 D1 discloses a method and a device for sending a certificate from a client to a server by inserting a certificate into a cookie header of a request in HTTP or equivalent protocol. D1 does not give any hint about how to ensure that the client is the authenticated owner of the certificate. The present solution consists then in

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT - SEPARATE SHEET**

International application No. PCT/EP2004/050864

providing a digital signature generated over a hash value of the request header with the client's name and client's public key as the authentication information to be inserted in the header request.

3. The dependent **claims 2-6, 8, 9, 11, 12, 14, 16** add further features to the subject-matter of the claims they depend on, and are therefore based on the same inventive concept.

4. Therefore **claims 1-16** are new and inventive.

21-04-2005.

14 April 2005

- 3 -

EP0450864
DE920030011 / EP2004/050864

modifications on the server side as well as the client side, e.g. additional card reader with specific security applications. Therefore, such implementations cause much effort on costs and time with the consequences that preferably only new client-server infrastructures will be using the digital signature procedure. The existence of those two authentication procedures in the client-server environment has the disadvantage that a client has to check at first whether the destination server is supporting the password logon or the digital signature procedure. Depending on that result the client will use the required authentication process supported by the server. It causes much unnecessary network traffic between client and server since the server application itself finally determines the type of authentication.

Furthermore, the present digital signature authentication procedures have the disadvantage that several screens between client and server have to be exchanged between client and server until the client can provide its authentication information. This causes much unnecessary network traffic.

US2002/0133700 A1 discloses a method and system for communicating a certificate between a security module and a server. The problem posed by the present invention is the lack of means for communicating a certificate from a client between a security module and a server, the protocol used between the client and the server being HTTP or an equivalent protocol, a security protocol like SSL or an equivalent protocol being implemented between the client and the security module. It offers a method and a device for communicating said certificate from the module to the server, which consists of inserting said certificate into a cookie header of a request in HTTP or an equivalent protocol sent by the client.

21-04-2005

14 April 2005

- 3a -

DE920030011 / EP2004/050804

EP0450864

Object of the invention

Starting from this, the object of the present invention is to provide a method and system for authenticating clients in a client-server environment by avoiding the disadvantages of the above-mentioned prior art.

Brief summary of the invention

The idea of the present invention is to replace the existing password/user ID based authentication process by a new digital signature authentication process in which preferably the first

C L A I M S

1. Method for authenticating clients in a client-server environment, wherein said client-server environment uses a communication protocol that allows extensions of the header request without violating said communication protocol, wherein said client comprises the steps of:

generating a header request(10),

inserting client authentication information into said header request resulting in an extended header request (20)

independently of the authentication process used by said server and without server requesting authentication information, wherein said authentication information comprises the client certificate containing client's name and client public key, and a digital signature which has been generated over a hash value of the header request including client certificate using Client private key,

sending said extended header request to a server (30),

and receiving information from said server if authentication has been successful (35,60).

2. Method according to claim 1, wherein said communication protocol is a HTTP-protocol.

3. Method according to claim 1, wherein said authentication information is included in the first header request for establishing a session with said server.

4. Method according to claim 1, wherein said authentication information is automatically inserted into said header request by the Client's browser.

5. Method according to claim 4, wherein said client browser receives said authentication information from a smart card (10) via a smart card reader.

6. Method according to claim 1, wherein said authentication information is automatically inserted into said header request by a client signature component (20) which receives said authentication information from a smart card (10) via a smart card reader.

7. Method for authenticating clients (1a, 1b) in a client-server environment, wherein said client-server environment uses a communication protocol that allows extensions of the header request without violating said communication protocol, wherein a system (22) establishes communication between said client (1a, 1b) and said server (3), wherein said system(22) comprises the steps of:

receiving a header request from said client(1a,1b),

inserting authentication information into said header request resulting in an extended header request(20) independently of the authentication process used by said server and without server requesting authentication information, wherein said authentication information comprises the client certificate containing client's name and client's public key, and a digital signature which has been generated over the whole header request including client certificate using Client's private key,

sending said extended header request to a server (3), and

receiving information from said server (3), if the authentication has been successful.

8. Method according to claim 7, wherein said system (20) can be a proxy server, a gateway, or a tunnel.

9. Method according to claim 7, wherein said communication protocol is the HTTP-protocol, and said authentication information is automatically inserted into said HTTP-request header by said an insertion component (20) which receives said authentication information from a signature component (24).

10. Method for authenticating clients in a client-server environment, wherein said client-server environment uses a communication protocol that allows extensions of the header request without violating said communication protocol, wherein at said server side said method comprises the steps of:

receiving a client header request containing authentication information, wherein said authentication information comprises the client certificate containing client's name and client's public key, and a digital signature which has been generated over the whole header request including client certificate using Client's private key,

validating said authentication information contained in said header request by said-server authentication component, and

providing information to said client, if the authentication has been successful.

11. Method according to claim 10, wherein said communication protocol is the HTTP-protocol, and said authentication component performs the steps of:

accessing said public key contained in the client certificate, decrypting said digital signature contained in the HTTP-request header with said public key resulting in a hash value, applying the same hash algorithm as used by said client to said HTTP-request header, and considering authentication as successful, if both hash values match.

12. Server System (3) for authenticating clients (1) in a client-service environment, wherein said client-server environment uses a communication protocol that allows extensions of the header request without violating said communication protocol, wherein said client (1) provides authentication information in the header request to said server system, wherein said server system (3) comprising:

an authentication component (4) with the functionality to read said authentication information contained in the incoming client header request, wherein said authentication information comprises the client certificate containing client's name and client's public key, and a digital signature which has been generated over the whole header request including client certificate using Client's private key, and to validate said authentication information without having requested said authentication information from said client.

13. Client System (1) to be authenticated by a server system in client-server environment, wherein said client-server environment uses a communication protocol that allows extensions of the header request without violating said communication protocol, wherein said client system comprising:

a browser (2), and

a component for inserting client authentication information into said header request independently of the authentication process used by said server and without server requesting authentication information, wherein said authentication information comprises the client certificate containing client's name and client's public key, and a digital signature which has been generated over the hash value of the header request content using Client's private key.

14. Client System according to claim 13, further comprising a smart card reader (10), and a smart card (10) with a security module containing client's private key and a client certificate containing client name and private key, wherein said smart card provides said certificate together with a digital signature to said inserting component, wherein said digital signature is the result of an encryption of a hash value of said header request containing said certificate information by means of said private key.

15. Proxy Server system (22) for providing client authentication information to a server system (3), wherein said proxy server system (22) has a communication connection with a client system

21-04-2005

14 April 2005

- 5 - DE920030011 / EP2004/050864

EP0450864

(1a, 1b) and a server system (3), wherein said communication protocol used between said systems allows extensions of the header request of said header request without violating said communication protocol, wherein said proxy server system (22) comprising:

a proxy insertion component (20) for inserting the client certificate and digital signature into the header request received from said client independently of the authentication process used by said server and without server requesting authentication information, and

a signature component (24) for creating a digital signature and for providing it together with said client certificate to said proxy insertion component (20).

16. Computer program product stored in the internal memory of a digital computer, containing parts of software code to execute the method in accordance with claim 1-11 if the product is run on the computer.